

互联网法律白皮书

（2020 年）

中国信息通信研究院

2020年12月

版权声明

前　言

过去一年，新冠肺炎疫情在全球蔓延，冲击了世界经济和社会发展秩序，对互联网法治建设产生了深刻的影响。利用大数据防控疫情既取得了积极成效，也导致个人信息滥用、泄露问题进一步凸显，主要国家和地区通过制定立法和指南的方式进一步加强了对个人信息的保护。后疫情时代，国际范围内互联网与传统经济社会加速融合，网络安全、内容治理等问题日益严峻，线下治理向线上治理转型趋势明显。

我国互联网立法持续完善，过去一年，《民法典》《出口管制法》《数据安全法（草案）》《个人信息保护法（草案）》出台或公布，不断填补我国数据安全管理方面的空白，进一步构建从基础设施到应用、服务的网络安全管理框架；《网络信息内容生态治理规定》的出台，标志着网络内容管理从"两分法"向"三分法"转变；《未成年人保护法》新增"网络保护"专章，网络社会法治规范趋于体系化。同时，互联网执法、司法整体水平不断提高。党的十九届五中全会发布了《"十四五"规划建议》，明确加强重点领域、新兴领域、涉外领域立法，为下一步互联网法治建设指明了方向。

在往年的基础之上，中国信息通信研究院编制了《互联网法律白皮书（2020 年）》，希望为社会各界提供参考。

目 录

一、国外进展

过去一年，新冠肺炎疫情在全球范围内蔓延，对世界经济秩序造成了较大冲击。疫情期间，稳定高效的信息通信、个人信息的深度分析、治疗手段的数字建模等信息化应用手段成为了抗击疫情的重要构成。疫情期间的信息技术应用创新带来的虚假信息传播、个人信息滥用等新挑战和新问题，在网络数据安全、网络内容管理、网络社会规范等方面形成新的关注点。相关国家和地区为应对上述问题，通过加强数据治理、推进内容管理、强化平台责任、规范网络社会等方式积极应对，以保障国家安全、维护社会稳定、保护个人权益。

（一）网络安全持续升温，聚焦数据安全

网络安全一直是互联网时代各国关注的重要问题。近年来，随着数字经济的发展，数据作为生产要素的地位越来越凸显，新技术新业务的应用和创新离不开大数据的收集和使用。个人信息保护问题仍然广泛受到关注，而对更宽泛意义的数据资源的争夺已经开始，逐渐向网络主权、数据主权层面提升，数据博弈斗争愈发激烈。数据泄露、数据攻击、数据跨境等数据安全问题不断形成焦点。各国在对传统网络安全进行规制的同时将更多的关注点聚焦于数据安全领域，主要国家和地区从自身国情出发，积极部署国家安全战略、数据战略，强化数据风险控制，抢占数字经济发展先机。部分国家通过立法、指南等方式规范个人信息利用和保护，开展数据执法司法活动，落实数据安全保障。

1.部署国家安全规划，强化风险管控措施

网络安全是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，是信息技术时代各国关注的重点内容之一。过去一年，主要国家围绕基础设施、供应链安全积极部署，全方位巩固网络整体安全，同时积极利用网络技术手段加强保障水平。**一是关注基础设施安全，**2020 年 1 月，爱尔兰政府发布《2019-2024 年国家网络安全战略》，描绘了安全可靠网络空间的愿景，提出了发展国家网络安全中心的路线图，强调提高国家关键基础设施和公共服务的稳定性。2 月，美国总统特朗普签署《关于加强负责任使用定位、导航和授时服务以增强国家弹性的行政令》[1]，要求联邦各部门采取措施防止依赖于定位、导航和授时服务（PNT）的关键基础设施受到干扰和操纵，这是美国第一部关于 PNT 应用的行政令。**二是关注供应链安全，**2020 年 9 月，《美国在更具生产力的新兴科技经济中的竞争力法案》特别针对确保供应链安全提出了要求；波兰政府公布了《网络安全法（草案）》，按照潜在威胁程度将网络供应商分成四个组，衡量标准是供应商是否可能受到欧盟或北约组织以外国家政府的影响，以及供应商所在国家是否尊重人权等，通信运营商不得采购被视为是“高风险”供应商的新设备，而且必须在五年内更换从这家供应商购买的现有通信设备。10 月，葡萄牙政府表示将通过一项法律，要求电信设备供应商证明其安全，且将针对高风险供应商发布禁令。11 月，英国议会提出《电信（安全）法案》，明确赋予政府前所未有的新权力，以提

[1] Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services.

高英国电信网络的安全标准，并消除高风险供应商的威胁，其根本目的在于限制英国的电信公司使用华为设备。如果违反禁令，电信公司将被处以罚款。**三是积极利用网络技术手段助力保障国家安全。**2020年 1 月，俄罗斯议员提出打击网络犯罪法案，拟授权俄罗斯银行通过俄罗斯联邦通信、信息技术和大众传媒监督局（Roskomnadzor）直接封锁站点，以防止和打击网络诈骗。4 月，美国发布行政令成立美国通信服务业外国参与审查委员会，协助联邦通信委员会（FCC）对由外国参与引起的涉及公众利益的国家安全和执法问题进行审查评估，以保障通信网络安全。8 月，英国发布《自由保护法 2012》[2]的指南修订案，允许警察部队基于国家安全目的保留和使用生物识别信息。

2.出台国家数据战略，抢占数字经济先机

随着人类进入数字化时代，世界各国对数据的依赖快速上升，为争夺数据资源，维护本国数据主权，助力本国数字经济发展，欧美各国积极出台数据战略，提出数据愿景，明确本国的数字经济发展总体定位和规划。2019 年 12 月，美国推出《联邦数据战略与 2020 年行动计划》[3]，描述了美国联邦政府自 2020 年起未来十年的数据愿景，确定了在国家层面营造数据驱动的文化氛围，主要从标准、工具包、伦理框架等多层面促进数据共享，并推动形成数据使用的可问责性和透明度理念。2020 年 2 月，欧盟委员会发布《欧盟数据战略》[4]，在数据市场公平性、数据互操作性、数据治理、数据的个人控制权等方面积极推进数字化转型工作，旨在打造欧盟单一数据市场，强化技术

[2] Protection of Freedoms Act 2012.
[3] 2020 Action Plan for the Federal Data Strategy.
[4] European Strategy for Data.

主权，提升企业竞争力，以期在新一轮数字革命中后发制人。9 月，英国发布《国家数据战略》[5]，阐明了如何在英国释放数据的力量，建立了通过数据促进经济发展的框架，旨在通过数据使用推动经济增长、改善社会公共服务，使英国成为下一轮数据驱动型创新的领导者。

3.全面保护个人信息，立法指南双线并进

个人信息保护一直是全球的热点话题。过去一年，各国通过数字化手段开展疫情防控，个人信息滥用、泄露的问题更加凸显。在此背景下，许多国家的个人信息保护立法进程同步加快。同时，已经制定了个人信息保护立法的国家和地区，将个人信息保护的工作聚焦到了根据形势需要修订立法和出台更加细化的指南方面。**一方面，制定新的个人信息保护立法。**2020 年 1 月，印度尼西亚总统正式向众议院提交了《个人数据保护法》[6]草案。2 月，澳大利亚公平竞争和消费者委员会（ACCC）发布《竞争与消费者（消费者数据权）规则》[7]，保证个人能够便利访问、企业能够高效处理消费者数据；北马其顿共和国参照欧盟《通用数据保护条例》（GDPR）制定了《个人信息保护法（2020）》[8]，只在个别规定有所差异。6 月，牙买加参议院通过了《数据保护法》，为政府、企业和组织如何正确收集、存储和处理个人数据制定明确的准则，该法将于 2022 年生效。11 月，加拿大创新、科学和工业部提出了新的数据保护法规《数字宪章实施法》[9]，旨在适应数字时代需要，更好保护加拿大人的隐私，该法将大幅提高罚款

[5] National Data Strategy.
[6] Personal Data Protection Act.
[7] Computation And Consumer(Consumer Data Right)Rules 2020.
[8] Personal Data Protection Act（2020）.
[9] Digital Charter Implementation Act.

额度，最高罚款可达全球收入的 5%或 2500 万加元（两者取其高）。**另一方面，修改现行立法和出台指南细化解释现行立法。**2020 年 2 月，韩国对《信息通信网络的利用促进与信息保护等相关法》[10]《个人信息保护法》[11]《信用信息的利用与保护法》[12]等个人信息保护相关法律作出大范围修订，将个人信息保护相关规定内容整合到《个人信息保护法》中，以解决有关人员混乱、重复监管等问题。5 月，新加坡通信信息部（MCI）和个人数据保护委员会（PDPC）联合发布了《个人数据保护法（修订）》草案[13]，加强机构问责制，对个人的同意作出更加详细的规定。6 月，新西兰通过了对 1993 年《隐私法》[14]的修订，加强了个人信息保护监管机构的权力，规范了数据跨境流动以及数据违规报告制度；日本通过《个人信息保护法（修订）》提案[15]，对个人权利、经营者的义务以及数据利用制度等进行了修订。8 月，韩国公布了《个人信息保护法》执行令修订案[16]，明确了个人信息追加利用或转移的标准，扩大了敏感信息的范围；美国出台了《加州消费者隐私法实施条例》[17]，主要是为法律适用的准确性、一致性和明确性进行了非实质性的变动。欧盟数据保护委员会（EDPB）在过去一年发布了《疫情背景下用于研究目的的健康数据处理指南》《关于第二支付服务指令和 GDPR 相互影响的指南》《针对社交媒体用户的

[10] 정보통신망 이용촉진 및 정보보호 등에 관한 법률.
[11] 개인정보 보호법.
[12] 신용정보의 이용 및 보호에 관한 법률.
[13] Personal Data Protection（Amendment）Bill 2020.
[14] New Zealand Privacy Act 1993.
[15] 個人情報の保護に関する法律等の一部を改正する法律。
[16] 《개인정보 보호법》 시행령 개정안.
[17] California Consumer Privacy Act Implementation Regulations.

指南》《数据控制者和处理者概念解释的指南》等文件，以进一步明确 GDPR 的适用。

4.完善数据安全保障，开展数据执法司法

过去一年，主要国家和地区围绕数据安全保护，针对大型互联网企业、大型产品和服务提供商、政府机构等重点主体多方面多层次开展执法司法活动，主要关注点聚焦于生物识别数据、数据的滥用行为、数据主体的权利实现、数据跨境流动等问题。**一是关注生物识别数据的处理行为，通过执法司法活动限制处理范围，明确处理要求。**2020 年 7 月，英国信息专员办公室（ICO）和澳大利亚信息专员办公室（OAIC）对美国面部识别软件提供商 Clearview AI 的个人数据处理活动展开了联合调查。8 月，英国南威尔士上诉法院推翻了英国“人脸识别首案”的判决，明确英国警方在辖区街道使用自动面部识别技术抓取用户面部数据违反《数据保护法》[18]，侵犯了原告的隐私权等合法权利。**二是对数据收集、使用、共享等违规滥用行为进行调查。**2020 年 3 月，针对脸书-剑桥分析滥用用户数据事件，澳大利亚信息专员办公室（OAIC）以违反隐私法为由对其提起诉讼。9 月，法国 CNIL 针对一位政府官员违规将国家档案局中的高中生数据传输给他人的行为展开调查，认为该官员的滥用个人数据行为违反了 GDPR 对于个人数据使用目的的规定。4 月，爱尔兰数据保护委员会请求欧盟数据保护委员会（EDPB）就远程会议软件服务提供商 Zoom 的隐私和安全问题进行调查。**三是对侵犯用户数据权利及未履行数据安全**

[18] Data Protection Act.

保障义务的行为进行执法处罚。2020 年 1 月，欧洲手机零售商迪克森公司（Dixons Carphone）因遭受网络攻击导致黑客窃取了 1400 万人的个人信息，英国信息专员办公室（ICO）对其处以 50 万英镑的罚款。3 月，谷歌由于没能实现用户的被遗忘权请求，瑞典数据保护局（Datainspektionen）对其处以 7500 万瑞典克朗的罚款。7 月，由于谷歌公司未能充分处理比利时公众人物提出的删除权请求，比利时数据保护局（APD）对其处以 60 万欧元罚款；韩国通信委员会（KCC）认为 TikTok 对儿童用户数据进行不当处理，对其作出 1.86 亿韩元罚款。12 月 7 日，法国国家信息与自由委员会（CNIL）决定分别向谷歌和亚马逊开出 1 亿欧元和 3500 万欧元的罚单，理由是法国谷歌和亚马逊网站存在违规使用 Cookies 的情况。**四是数据跨境流动的多双边机制在复杂国际形势下变化明显**。2020 年 7 月，欧盟最高司法机构欧洲法院认为欧美“隐私盾协定”[19]对于欧美间数据跨境未达到 GDPR 要求的“充分保护”标准，裁决该协定无效。欧盟支持法院判决，但并不意味着数据跨境被完全禁止。欧洲数据保护主管（EDPS）重申了坚持对从欧盟转移到第三国的个人数据进行高度保护的重要性。对于向第三国进行的个人数据传输，欧盟数据保护委员会（EDPB）表示会提供进一步说明和指南。德国数据保护机构（DSK）指出仍然可以进行国际数据传输，但必须尊重欧洲公民的基本权利。美国表示希望与欧洲加强合作以减少“隐私盾协议”失效对美欧经济关系造成的负面影响。11 月，东盟十国、中国、日本、韩国、澳大利亚、新

[19] EU-U.S.Privacy Shield.

西兰等 15 个国家经贸部长正式签署《区域全面经济伙伴关系协定》（RCEP），标志着世界上人口数量最多、成员结构最多元、发展潜力最大的东亚自贸区建设成功启动。RCEP 涉及货物贸易、服务贸易、投资、电子商务、知识产权等多个方面，其中明确了电子商务项下各成员方制定数据本地化和数据跨境流动政策的基本原则，为全球实现数据跨境流动破局、构建数据跨境流动体系提出了亚洲方案。

（二）内容管理更加强化，突出平台责任

仇恨言论、恐怖主义内容一直是欧美主要国家和地区在互联网立法中关注的重点。过去一年，在新冠肺炎疫情全球蔓延的背景下，网络上针对疫情的虚假信息、虚假新闻等负面内容频发，不仅带来了社会恐慌，而且扰乱了各国政府发布疫情相关信息、开展疫情防控的行动，引发了国际社会对网络内容管理的高度重视。

1.平台责任不断丰富，各国制定修订立法

为增强网络内容管理力度，主要国家和地区以制定、修改立法的形式对平台内容管理义务进行增补。部分国家立法给网络平台增加了新的义务类型。2020 年 2 月，德国发布《打击右翼极端主义和仇恨犯罪》[20]的法律草案，对现有的《网络执行法》[21]进行了修订，增加了社交平台的报告义务；巴基斯坦出台了《保护免受在线伤害的规则》[22]，规定社交媒体公司有义务协助执法机构获取相关信息，并将非法的网络信息内容移除。7 月，土耳其议会批准了《媒体法》[23]修改案，

[20] Gegen Rechtsextremismus und Hasskriminalitä.
[21] Netzwerkdurchsetzungsgesetz.
[22] Citizens Protection (Against Online Harm) Rules.
[23] Social media law.

规定了社交平台在本地设立代表处的义务。**部分国家立法对网络平台既有的权利义务类型进行了调整。**2020 年 9 月，欧盟制定《数字服务法案》[24]，主要内容之一就是对在线社交媒体平台处理非法内容、虚假信息方面的责任和义务作出新的规定，同时明确网络平台删除内容或产品的决定必须是透明的，以确保合法的产品和服务不会被删除；美国司法部提出新立法草案，准备修订长期处于争议状态的美国《通信规范法》[25]“230 条款”，规定当平台存在有意传播或参与违反联邦刑法的内容制作，或已经注意到平台上的违法内容但是没有迅速删除、也没有及时向执法部门报告等情形的，将承担法律责任。

2.关注儿童在线保护，维护健康网络环境

儿童网络保护是网络内容管理领域的重点，过去一年得到不断增强。通过立法加大保护力度。2020 年 1 月，爱尔兰政府发布《在线安全和媒体法案》[26]，规定成立新的媒体委员会，保护儿童的利益，使其免受不良信息侵害。5 月，韩国发布了《保护儿童和青少年性行为法（修订）》[27]，加强了信息通信从业者的责任，以增加对于未成年人的保护力度，防止“N 号房”事件再次发生。**细化儿童网络保护领域的规范指引。**2020 年 4 月，英国信息专员办公室（ICO）发布了关于网络服务的《适龄设计实践守则》[28]的最终版，为儿童在线隐私与安全提供指引。6 月，国际电联（ITU）发布新版《2020 年保护上网

---

[24] Digital Services Act.
[25] Communications Decency Act.
[26] Online Safety and Media Regulation Bill.
[27] 아동・청소년의 성보호에 관한 법률.
[28] Age Appropriate Design Code.

儿童指南》[29]，供儿童、家长和教育工作者、政策制定者参考，内容涉及如何为儿童和青少年创造一个安全的在线环境。**加强儿童网络保护领域的执法力度**。2020 年 9 月，荷兰政府采取严厉措施打击线上伤害儿童的行为，将“不良或管理松懈”的网络托管公司列入黑名单。

（三）网络社会不断规范，应对新旧问题

过去一年，新型数据不正当竞争行为和垄断行为涌现，人工智能、5G 和生物识别等技术应用带来的负外部性溢出。为维持网络空间良好社会秩序，主要国家和地区调整监管机制、完善立法，积极应对，规范网络社会秩序。

1.规范网络市场秩序，丰富监管机制手段

过去一年，在互联网竞争方面，主要国家和地区对大型互联网企业的关注更加凸显，规制重点除传统的价格竞争等行为外，逐步向数据领域集中。**一方面，在新型数据不正当竞争行为和垄断行为不断出现的背景下探寻切实有效的监管新机制**。2020 年 4 月，法国竞争管理局（ADC）裁定，谷歌的内容服务为法国出版行业带来严重损害，危及了整个行业的经济状况，谷歌必须就法国出版公司和新闻机构的内容付费；澳大利亚联邦政府指示澳大利亚竞争和消费者委员会(ACCC)制定强制性行为守则，规范数据共享、在线新闻内容排名以及分享新闻收入等问题。9 月，德国政府修订《竞争数字化法案》，确保平台竞争对手公平获得市场和数据访问权。**另一方面，关注传统的市场竞争和垄断行为**。2020 年 6 月，欧盟委员会推进《数字服务

[29] 2020 Guidelines on Child Online Protection.

法案》[30]，规定若科技巨头的市场主导地位被认为威胁到客户和较小竞争对手的利益，则将迫使它们分拆或出售部分欧洲业务。9 月，俄罗斯联邦反垄断局（FAS）认为，缤客（Booking）网站禁止旅馆提供比旅馆与公司之间商定价格更优惠的价格的行为，违反俄罗斯《反垄断法》[31]。

2.发展新技术新应用，形成配套制度保障

随着数字经济的发展，高新科技在经济发展中的重要地位日渐提升，各国争相通过投资、制定政策和制度配置等方式推动新技术新业务在规范中发展，以在全球竞争中取得优势地位。

在人工智能领域，主要国家和地区的态度还是以鼓励应用、促进发展为主，同时通过指南等方式进一步明确产业要求，促进人工智能技术在规范中统一和发展。**在鼓励利用方面，**主要借助人工智能生态建设、产业促进计划和人才战略等手段进行部署。2020 年 5 月，韩国国会通过一项修订法案，将现行的《国家信息化基本法》[32]修改为《基本智能信息法》[33]，以建立一个在法律体系下引领世界的人工智能生态系统。6 月，美国国会酝酿制定《军队人工智能法》[34]，进一步鼓励国防部使用人工智能技术，实施人工智能人才战略。**在精准监管方面，**主要通过指南等“软法”手段规范新技术新应用发展。2020 年 1 月，美国白宫发布了《人工智能应用监管指南备忘录（草案）》[35]，

[30] Digital Services Act.
[31] Антимонопольный закон.
[32] 국가정보화 기본법.
[33] 지능정보화 기본법.
[34] Artificial Intelligence for the Armed Forces Act.
[35] Guidance for Regulation of Artificial Intelligence Applications.

该备忘录从监管和非监管层面提出了人工智能应用相关原则和建议。2 月，英国信息专员办公室（ICO）发布《人工智能审查框架指南》[36]，为审计人工智能应用程序以及确保公平处理个人数据提供了可靠的方法。

在 5G 领域，各国通过增大技术研发投入、拓宽产业应用渠道等方式促进发展。**一是发达国家通过加强盟国合作、出台支持法案等方式维护在技术和标准方面的领先地位。**2020 年 1 月，美国众议院通过了两项促进 5G 和无线领域建设的法案，明确了美国要在下一代移动电信系统和基础设施的国际标准制定机构中保持领导地位。2 月，日本出台一项法案，支持企业开发安全的 5G 移动网络和无人机技术。**二是发展中国家积极探索适合本国利益的 5G 发展道路。**2020 年 8 月，罗马尼亚公布了 5G 网络立法草案，要求采取措施保护符合国家利益的信息和通信基础设施建设，并规定了实施 5G 网络的条件。

在生物识别信息利用领域，专项立法的需求渐增，部分国家开始推进人脸识别立法，尝试为使用人脸识别技术建立较高的法律门槛。**一方面，重点关注对公共部门使用人脸识别技术的限制。**2020 年 2 月，美国参议院提出了《道德使用人脸识别法案》[37]，要求在未形成政府使用准则前暂时禁止政府机构使用人脸识别。3 月，苏格兰议会通过《生物识别技术专员法案》[38]，要求在政府中设立生物识别技术专员，以监督苏格兰警方如何获取、存储、使用和处置生物识别数据。6 月，由弗洛伊德之死引发的对于警察使用人脸识别技术手段进行权

[36] Guidance on the AI auditing framework.
[37] Ethical Use of Facial Recognition Act.
[38] Scottish Biometrics Commissioner Act 2020.

力限制的讨论，美国明尼苏达州联合立法委员会考虑制定规范企业和政府使用面部识别技术的立法。**另一方面，积极探索人脸识别技术的使用标准。**2020 年 2 月，欧盟出台《人工智能白皮书》[39]，计划针对生物识别技术制定明确的标准。3 月，世界经济论坛（WEF）发布《负责任地使用人脸识别技术的政策框架》[40]，提出了具体的方案和步骤。

3.数字税开征再兴起，相关立法纷纷启动

大型互联网企业在低税率地区避税，税负不公平现象显著，部分国家及国际组织开启国际税制改革谈判，数字服务征税相关立法纷纷启动。目前，近 140 个国家和地区正在就国际税法的修改问题进行谈判，多个国家试图通过经济合作与发展组织（OECD）框架就如何对跨境互联网企业征收数字税达成多边协议，部分技术输入国企图通过征收数字税的形式谋求利益分羹。法国、新加坡、马来西亚、印度、菲律宾、印度尼西亚和泰国等国已通过或者已实施开征数字税的法案。其中法国表示，将从 2020 年 12 月起对全球数字业务年营业收入超过 7.5 亿欧元、同时在法国境内年营业收入超过 2500 万欧元的高科技企业征收 3%的数字服务税。作为数字税的主要被征收方，美国开始对欧盟、英国、意大利、巴西、印度等 10 个贸易伙伴已执行或拟征收的数字税发起“301 调查”，对各国征收数字税行为进行反制。

二、国内进展

过去一年，我国互联网法治进程持续加快，网络安全、网络内容管理、网络社会领域法治化程度进展明显。从传统网络安全问题转向

39 White Paper on Artificial Intelligence.
40 The Framework for Responsible Limits on Facial Recognition.

数据安全问题的趋势非常突出，《民法典》《数据安全法（草案）》《个人信息保护法（草案）》等涉及保护数据安全的关键立法相继制定出台或公布；为营造良好网络生态，《网络信息内容生态治理规定》采取“三分法”形式明确对违法和不良网络信息的治理，执法活动不断强化平台责任监管；同时，针对未成年人网络保护、网络犯罪、市场秩序等网络社会问题的立法、执法、司法体系也进一步完善。

（一）数据安全顶层设计明确，网络安全制度细化

我国在关注网络安全的基础上更加注重国家整体数据安全治理，通过顶层设计和配套立法的方式，充实法律依据，提高具体可操作性。

1.数据安全顶层设计加快推进

随着数字化和全球化进程的不断加快，数据在提振一国整体数字经济发展中发挥着不可估量的作用，数据安全问题在国家整体安全中的重要性更加凸显。各类数据活动的全方位融合普及和多样的数据处理需求，催生了大量新发展机遇，但同时也带来了大量的数据安全风险。以创新为主要引领和支撑的数字经济需要完善的数据安全治理体系来消除数据风险、保障数字经济安全。

2020 年 6 月，十三届全国人大常委会第二十次会议对《数据安全法（草案）》进行了审议，7 月，《数据安全法（草案）》公布，向社会公开征求意见。《数据安全法（草案）》共 7 章 51 条，对保护数据安全进行了顶层设计：**一是**明确国家安全领导机构的决策和统筹协调职责，加强对数据安全工作的组织领导；**二是**对数据安全与发展的措施作了专章规定，促进以数据为关键要素的数字经济发展；**三是**为

应对境内外数据安全风险，明确建立健全国家数据安全管理制度，完善国家数据安全治理体系。**四是**明确开展数据活动的组织、个人的数据安全保护义务。**五是**明确推动政务数据开放和利用的保障措施。《数据安全法》的制定为数据安全治理有法可依、有章可循奠定基础，体现出国家在保障数据安全、维护国家数据主权方面的决心，在监管机构的职责明确、数据安全保障能力提高、数据安全和自由流动促进等方面具有重要的里程碑意义。

2020 年 10 月，十三届全国人大常委会第二十二次会议审议通过的《出口管制法》明确了对特定物项（包括特定物项的技术资料等）出口实施许可制度，在总结出口管制经验和借鉴国际通行做法基础上，以出口管制的形式明确了我国重要数据的出境要求，补充完善了国家整体数据安全制度。

2.网络安全审查具体要求落地实施

网络安全审查是依据《网络安全法》开展的一项重要工作。《网络安全法》第三十五条规定，“关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查”。2020 年 4 月，国家网信办等 12 个部门联合发布《网络安全审查办法》，并于 6 月 1 日起正式实施。**该办法以体制机制建设为前提，明确了网络安全审查的审查对象、审查重点、审查流程等主要内容：**明确了国家网信办牵头、多部委参与的网络安全审查体制机制，反映了网络安全审查涵盖关键信息基础设施行业、领域的跨部门特点；规定了申报者的范围是在采购网络产品

和服务时，影响或可能影响国家安全的关键信息基础设施运营者；明确审查的重点为关键信息基础设施存在被非法控制、破坏，以及重要数据被窃取、泄露、毁损等风险的情况；明确了具体的申报和审查流程，以及关键信息基础设施运营者对于网络安全审查的预判和配合义务、审查者的保密义务等相关内容。该办法坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务安全性、可能带来的国家安全风险等方面进行审查，为我国开展网络安全审查工作提供了重要的制度保障。

（二）个人信息保护立法加快，执法司法同步推进

个人信息保护问题目前仍然是我国互联网法治建设中的重点内容。截至 2020 年 6 月，我国互联网用户已达 9.4 亿，互联网网站超过 400 万个、应用程序数量超过 300 万个，个人信息的收集、使用活动更为广泛。虽然近年来我国个人信息保护力度不断加大，但在现实生活中，随意收集、违法获取、过度使用、非法买卖个人信息，利用个人信息侵扰人民群众生活安宁、危害人民群众财产安全和生命健康等问题仍十分突出。过去一年，我国相关部门在推动科学立法、严格执法、精细司法方面不断发力，进一步推动我国个人信息保护水平持续提高。

1.立法强化个人信息权益保护

2020 年在我国个人信息保护工作中具有里程碑意义，《民法典》完善了民事领域个人信息权益的保护，《个人信息保护法（草案）》的

公布开启了我国个人信息保护领域统一立法的元年，两部立法分别从民事角度和行政角度明确了个人信息保护的具体规则。

一是个人信息的定义不断完善。《网络安全法》《民法典》都通过“概括+列举”的方式和“识别说”的模式规定了个人信息的内涵和外延。《民法典》在判断标准上与《网络安全法》基本一致，但在具体的列举中，增加了电子邮箱和行踪信息，同时在疫情防控的大背景下，特别考虑到了公民健康信息的重要性和敏感性，也通过明确列举的方式确认公民健康信息为个人信息。《个人信息保护法（草案）》明确个人信息是指与“已识别”或“可识别”的自然人有关的各种信息，与《网络安全法》和《民法典》规定的“单独识别和结合识别”的“识别说”相比，《个人信息保护法（草案）》也具备“关联说”的要素，同时删除了之前立法中对个人信息具体类型的列举。“能够识别”个人和与“自然人有关”的不同判断标准是否会对具体信息类型的定性产生影响还有待学界进一步探讨和司法实践的检验，但从本质来看，两种不同判断标准并不具有太大差别，只要与自然人有关的信息，无论是单独还是与其他信息相结合应当都能产生定位到个人的结果。

二是区分了隐私和个人信息。《民法典》延续了《民法总则》对隐私权和个人信息的进行区分的做法。隐私包含私人生活、私人秘密两个方面的内容，个人信息更加强调对自然人身份的识别性，两者存在“私密信息”这一交叉领域。“私密信息”既属于隐私又属于个人信息，具有隐私权的“不愿为他人知晓”的特征。

三是个人信息保护权利制度确立。《民法典》赋予了自然人知情、

查阅复制、请求更正、删除等权益。《个人信息保护法（草案)》在吸收借鉴国际立法权利制度设计经验的基础之上，扩展到知情权、决定权、限制处理权、查阅复制权、补充更正权、删除权等内容。

四是明确了处理个人信息的具体规则。《民法典》和《个人信息保护法（草案)》具有一致性，均以个人信息的收集、存储、使用、加工、传输、提供、公开等个人信息处理活动的全生命周期为基础，规定了以自然人或监护人知情同意为核心的信息处理原则。

五是明确职责分工，突出网信部门统筹协调作用。《个人信息保护法（草案)》明确了国家网信部门的统筹协调作用，负责个人信息保护工作的统筹协调和监督管理，同时规定国务院有关部门在各自职责范围内负责个人信息保护和监督管理工作。个人信息保护工作事项涉及各行业各领域各类主体，事项众多、复杂度高，在互联网与各行业高度融合背景下，工作难度也更大，需要由专门的机构负责此项工作。各国负责个人信息保护的机构大多数是中央层面层级较高、具有较强统领和协调性的机构，且职权涵盖个人信息保护各个事项，也反映了这一趋势。《个人信息保护法（草案)》中设置的监管模式仍以分行业监管为主，各部门只负责监管与其行业相关领域下的个人信息保护问题，如何避免监管交叉、监管冲突或监管空白地带的问题，仍有必要进一步论证和完善。

六是加大惩处力度，强化违法行为惩戒效果。《个人信息保护法（草案)》对违反本法规定行为的处罚及侵害个人信息权益的民事赔偿等作了不同等级的规定。行政处罚方面，罚款力度加大，在《网络

安全法》的基础之上，对情节严重的，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款。除罚款以外，对侵害个人信息权益的民事赔偿，按照个人所受损失或者个人信息处理者所获利益确定数额，上述数额无法确定的，由人民法院根据实际情况确定赔偿数额。

2.执法加强相关制度落实

个人信息保护严格执法是有效控制信息泄露、信息滥用等问题的有效举措，是维护公民合法权益的有力手段。过去一年，我国执法机构通过专项行动、严格执法等举措重点针对疫情期间危害个人信息权益以及多个APP违法违规收集使用个人信息的违法行为进行了整治，整体执法活动呈现以下趋势。

一是监管主体多元化。当前个人信息保护的监管仍然由网信部门综合协调，公安机关、工信部门、市场监督管理部门以及其他行业主管部门在各自职责范围内行使监督管理职责。公安机关和工信部门聚焦互联网领域的APP治理，根据《网络安全法》第22条第三款、第41条和第64条第一款，对APP主体违法违规收集、处理个人信息的行为进行处罚。2019年11月以来，公安机关加大打击整治侵犯公民个人信息违法犯罪力度，集中查处整改了100款违法违规APP及其运营的互联网企业，工业和信息化部目前已完成国内用户使用率较高的52万款APP的技术检测工作，责令1571款违规APP进行整改，公开通报437款整改不到位的APP，下架94款拒不整改的APP；市场监督管理部门聚焦消费者权益保护领域，依据《消费者权益保护法》

第 56 条，对未经消费者同意收集其个人信息以及发送商业性信息的行为进行处罚。2020 年 4 月，公安部网络安全保卫局启动“净网 2020”专项行动，其中配合疫情防控工作严厉打击“网络水军”借疫情发布虚假信息犯罪活动。

二是监管活动主动化。个人信息保护的监管执法由被动执法向主动执法转变。7 月，国家网信办、工业和信息化部、公安部、国家市场监管总局四部门启动 2020 年 App 违法违规收集使用个人信息治理工作。截止 2020 年 12 月 3 日，工业和信息化部已经连续通报了六批侵害用户权益的 APP，提出了整改以及进一步严厉处置的要求。

三是监管手段灵活化。2020 年 6 月，国家网信办指导北京市网信办，约谈新浪微博负责人，针对微博在蒋某舆论事件中干扰网上传播秩序，以及传播违法违规信息等问题，责令其立即整改；10 月，北京市网信办针对“网易新闻”、网易号跟评环节多次传播违法违规信息等问题约谈网易负责人。第三季度，全国网信系统依法查处网上各类违法违规行为，累计约谈网站 1211 家。

3.司法明晰相关立法要求

全面推进互联网精细化司法有助于更好诠释立法精神，完善整体互联网法治体系建设。我国相关立法对于个人信息保护的基本原则进行了规定和明确，但是对于实践中的很多问题仍没有给出确切的答案，互联网法院在审理具体案件过程中，从现行立法的规定和基本精神出发，对个人信息保护和大数据使用中的一些重点难点问题进行了回应，形成了具有现实指导意义的判决。

一是区分了隐私和个人信息。如何判断具体案例中涉及到的信息是否属于个人信息或者隐私，不仅是司法在个案中进行精准裁判的依据，会对立法的进一步解释和适用产生长远的影响，而且是关系到自然人合法权益和产业发展、企业运营的关键问题。2020 年 7 月，北京互联网法院对“黄女士与腾讯科技（北京）有限公司等网络侵权责任纠纷一案”的判决明确微信好友关系、读书信息由于包含了可以指向信息主体的网络身份标识信息，且包括读书时长、最近阅读、书架、读书想法等，能够反映阅读习惯、偏好等，因此属于个人信息。但从隐私的防御性权利和精神利益特征以及个人信息的积极利用可能和财产性利益特征角度进行区分，法院并没有将好友关系和读书信息纳入隐私范畴。2020 年 9 月，北京互联网法院在“校友录”头像被爬一案的判决中，也以隐私的“不愿为他人知晓”的“私密性”为标准，将涉案姓名、照片及其关联关系等信息排除在了隐私范围之外。

二是明确了对敏感个人信息的保护。《个人信息保护法》出台之前，我国相关立法中并没有设置敏感个人信息的保护制度，对于面部信息等敏感类型个人信息并没有规定强于一般个人信息的特殊保护规则。同时，实践中也存在很多在非必要情况下收集使用敏感个人信息的案例，对个人的隐私带来很大的风险。2020 年 11 月，被称为国内“人脸识别第一案”的杭州市民郭兵诉杭州野生动物世界有限公司一案宣判。杭州市富阳人民法院一审判决，动物世界删除郭兵办理年卡时提交的面部特征信息，赔偿郭兵合同利益损失及交通费共计 1038 元。该案判决的出发点并非对敏感个人信息的强化保护，而是强调个

人信息的收集要遵循"合法、正当、必要"的原则和征得当事人同意，在保护个人合法权益方面与正在制定中的《个人信息保护法》专门规定的敏感个人信息保护规则具有一致性。

三是平衡了自然人个人信息合法权益保护和企业合理使用个人信息之间的关系。个人信息保护问题中，保护自然人合法权益和促进企业合理利用个人信息是天平的两端，如何促使双方取得最大利益的权衡是在公开的个人信息使用中体现最为明显的问题。在"校友录"头像被爬案中，法院没有对作为第三方的百度公司施加实质上的审查和注意义务，而是将个人信息公开在全网的责任归于直接和故意违反个人授权的搜狐公司。这一认定符合《民法典》中规定的"使用自然人公开和合法公开的个人信息可以不承担民事责任"的基本精神，对于企业在合法合理前提下使用网络公开信息具有支持和促进作用，避免了对企业苛以过重的责任而阻碍网络产业的发展。

（三）网络内容管理不断强化，平台责任持续落实

为有效肃清网络不良风气、营造良好网络生态环境，针对网络违法和不良信息，过去一年，多个部门通过出台立法、严格执法进行严厉打击。

1.具体管理规定不断出台

随着网络新技术新业务的不断推陈出新，新型问题也不断出现，平台责任如何确定和划分成为新的挑战，具体业务平台的规范也出现空白。过去一年，针对信息内容管理问题突出、平台责任有待加强等问题，相关部委发布了针对音视频业务、直播营销业务的管理规定，

同时，在整体管理思路上做出了“两分法”到“三分法”的转变。2019 年 11 月，国家网信办、文化和旅游部、国家广播电视总局联合发布《网络音视频信息服务管理规定》，这是我国针对网络音视频信息服务领域的专门规定，及时回应了当前网络音视频信息服务及相关技术发展面临的问题，全面规定了从事网络音视频信息服务应当遵守的管理要求，尤其针对实践中利用深度学习、虚拟现实等相关技术提供网络音视频信息服务的行为明确了保障国家安全、维护社会秩序、保护个人信息的要求。2019 年 12 月，国家网信办公布了《网络信息内容生态治理规定》，这是我国在网络信息内容管理领域的一部重要立法，为促进网络信息内容生态健康有序发展提供了重要指引，突破性的将内容管理方式从“两分法”调整为“三分法”，明确依法规范和管理平台上的违法信息、防范和抵制不良信息传播，是网络信息服务提供者必须承担的社会责任，也是法律责任，为保护公民、法人和其他组织的合法权益，维护国家安全和公共利益提供了有力保障。2020 年 11 月，为应对近年来直播带货在飞速发展的同时带来的虚假宣传、质量低劣、售后无门等问题，国家网信办发布《互联网直播营销信息内容服务管理规定（征求意见稿）》，对直播营销平台、直播间运营者和直播营销人员等作出具体规范，适用范围涵盖了通过互联网站、应用程序、小程序等，以视频直播、音频直播等形式向社会公众推销商品或服务的活动。

2.执法强化网络平台主体责任承担

平台在网络内容治理中的地位角色及其承担的社会责任和法律

责任越来越受到社会和政府的关注。过去一年，针对没有履行法律义务，放任违法和不良内容在网上发布和传播的平台，相关政府机构进行了严厉打击。

清理直播平台低俗色情信息。2020 年 1 月，深圳市网信办会同市“扫黄打非”办公室集中约谈了 19 家网络直播平台负责人，就各平台存在的低俗色情等乱象，责成平台切实履行企业主体责任，全面整改，确保良好网络直播生态。6 月起，国家网信办、全国“扫黄打非”办等部门启动为期半年的网络直播行业专项整治和规范管理行动，依法依规对传播淫秽色情、严重低俗庸俗内容的违法违规网络直播平台，分别采取约谈、下架、关停服务等阶梯处罚。

整治平台虚假信息和不良内容。2020 年 7 月起，国家网信办重点针对商业网站平台和“自媒体”炒作热点话题、违规采编发布互联网新闻信息、散播虚假信息等网络传播乱象开展集中整治。整治工作分为六个方面，对象涵盖了商业网站平台、手机浏览器、“自媒体”、移动应用商店境内新闻类 APP、社交平台等主体。

依法规范网络平台传播秩序。2020 年 6 月，国家网信办指导北京市网信办，约谈新浪微博负责人，针对微博在蒋某舆论事件中干扰网上传播秩序，以及传播违法违规信息等问题，责令其立即整改，并严肃处理相关责任人，同时，要求北京市网信办对新浪微博依法从严予以罚款。

（四）未成年人网络保护有力，主要立法顺利出台

2020 年 10 月 17 日，全国人大常委会表决通过修订后的《未成

年人保护法》，并将于 2021 年 6 月 1 日正式施行。此次法律修订立足当前未成年人网络保护实际，增设“网络保护”专章，对近年来社会各界高度关注的未成年人网络保护问题作出专门规定，为我国未成年人网络保护工作提供了坚实的法律保障。

聚焦我国未成年人网络保护工作亟需解决的现实问题。近年来，媒体报道以及相关机构的调查报告显示，网络直播服务出现许多不宜未成年人观看的内容；未成年人巨额网络直播打赏导致家庭财产损失；未成年人网络游戏沉迷严重影响其身心健康。《未成年人保护法》坚持问题导向，立足于当前未成年人保护存在的薄弱环节和迫切需求，尤其是对网络信息内容管理、未成年人个人信息保护、网络欺凌以及未成年人网络沉迷等突出问题做出了全面规范，并增加了相应的法律制度设计。

构建完善的未成年人网络保护监管机制。监管体制是法律实施和执行的重要保障，也是未成年人网络保护的关键环节。此次《未成年人保护法》修订明确要求网信部门及其他有关部门应当加强对未成年人网络保护工作的监督检查，并规定了公安、新闻出版、教育、卫生健康、文化和旅游、电影、广播电视等部门在未成年人沉迷网络干预、网络信息内容管理等方面的具体职责。

建立各方主体协同共治的综合保护体系。未成年人网络保护是一项系统工程，未成年人需要政府、社会、学校、家庭共同承担责任，相互配合。在推进未成年人网络保护的过程中，行政管理并不是唯一的手段，教育、引导等手段的辅助性作用也十分重要。因此，“网络

保护”专章更加强调未成年人网络保护工作中的综合治理模式。尤其立法突出了监护人在协同治理中的重要地位，赋权其多手段实施未成年人网络保护。例如，要求监护人主动安装过滤软件和选择适用未成年人的信息服务模式；收集和处理未成年人个人信息应由监护人决定；要求监护人管理未成年人的网络使用时限；监护人对网络欺凌行为可以要求服务提供商采取干预措施。在确立监护人首要责任的同时，也规定其他主体要为其提供配合手段。例如，要求国家、社会、学校和家庭加强未成年人的教育，提升网络素养；相关政府部门要给未成年人和监护人提供家庭教育指导；网络服务提供者应当采取技术手段规范未成年人上网安全。

重点建设未成年人网络防沉迷机制。首先，立法规定了政府有关部门干预未成年人沉迷网络的共管机制，要求新闻出版、教育、卫生健康、文化和旅游、网信等部门应当定期开展预防未成年人沉迷网络的宣传教育，监督网络产品和服务提供者履行预防未成年人沉迷网络的义务。**其次，**明确了学校预防沉迷网络的职责，学校发现未成年学生沉迷网络的，应当及时告知其父母或者其他监护人，共同对未成年学生进行教育和引导，帮助其恢复正常的学习生活。**再次，**强化了监护人的监护责任，由家长做好自我表率，要求未成年人的父母或者其他监护人提高网络素养，规范自身使用网络的行为，加强对未成年人使用网络行为的引导和监督。**最后，**规定了网络产品和服务提供者预防未成年人沉迷网络的义务，明确要求网络游戏、网络直播、网络音视频、网络社交等服务提供者应当设置相应的时间管理、权限管理、

消费管理等功能，以便监护人行使监护职责干预未成年人沉迷网络。

未成年人网络保护法治建设有待进一步推进。《未成年人保护法》以法律形式夯实了我国未成年人网络保护的制度基础。政府协同监管机制的细化，企业责任落实等问题还有待在《未成年人网络保护条例》等配套法规的规定中进一步落实。

（五）网络社会整体运转有序，重点问题得以回应

过去一年，为加强和创新网络社会管理，我国通过立法、执法、司法等方式针对网络犯罪、数据竞争等问题予以重点规制。

一方面，强化对网络犯罪的查处。相关部门通过专项行动、联合整治等多种方式加大对网络犯罪的惩戒力度。**整治网络金融违法行为。**按照公安部统一部署，2020 年，地方公安机关已破获重大非法网络支付案件 15 起，涉案资金 540 亿余元，取得阶段性成果。5 月，公安部部署开展“云剑-2020”打击贷款类电信网络诈骗犯罪专项行动，各地共查处为贷款类电信网络诈骗犯罪团伙提供服务的违法 1069 短信平台 57 个。**严查网络赌博典型案件。**2020 年 2 月，公安部开展打击治理跨境赌博专项行动，综合运用多种手段，集中摧毁了一大批跨境赌博犯罪团伙及招赌吸赌网络，初步遏制了境外赌博集团的不法行为，打击治理跨境赌博工作取得明显成效。**打击侵犯知识产权犯罪行为。**针对侵犯知识产权的违法行为，公安部、市场监管总局等多个部门进行严厉查处。自 2019 年 5 月开始至今，全国各级版权执法部门会同网信、工信、公安等部门，围绕当前网络版权治理热点难点开展多个领域专项整治，通过删除侵权盗版链接、收缴侵权盗版制品等方

式，不断规范网络版权秩序。

另一方面，维护互联网市场竞争秩序。对于损害市场竞争的行为，相关部门在过去一年严格执法，规范司法，维护了市场环境，保障了消费者的合法权益。**打击网络虚假广告行为。**2020 年 4 月，因为利用广告做虚假宣传，北京京东世纪信息技术有限公司被工商部门罚款 20 万元。8 月，湖南省市场监管局对某景点通过网络进行虚假宣传的行为作出行政处罚，责令其停止发布虚假广告，并处罚款人民币 120000 元。**规范网络交易活动。**2020 年 10 月，市场监管总局公开发布了《网络交易监督管理办法（征求意见稿）》，从整体上明确了符合行业发展规律和业态监管规律的监管规则，同时对 VIP 会员自动续费、平台强迫商家“二选一”、消费者差评遭删除等热点问题进行了进一步规范；市场监管总局等 14 家监管部门联合开展 2020 网剑行动，集中整治网络市场经营秩序违法行为。**明确数据权益纠纷司法边界。**当前立法并没有针对数据的市场竞争问题进行明确，为清晰界定各方市场主体在数据竞争中的权益，互联网法院在具体案例中不断探索，为规范互联网竞争做出指导性判决。2020 年 6 月，杭州互联网法院在“腾讯公司不正当竞争纠纷一案”中，明确了网络平台对于其所控制的用户信息享有竞争权益，其他企业违法违规使用信息的行为构成不正当竞争。

三、未来展望

2020 年 10 月，党的十九届五中全会通过的《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建

议》（《"十四五"规划建议》）中明确提出要"坚持法治国家、法治政府、法治社会一体建设，完善以宪法为核心的中国特色社会主义法律体系，加强重点领域、新兴领域、涉外领域立法，提高依法行政水平"。12 月，中共中央印发的《法治社会建设实施纲要(2020-2025 年)》中也指出要"建立健全网络综合治理体系"。当前，我国在网络安全保护、网络信息服务、网络社会管理等重要领域的互联网法律框架初步构建完成，《网络安全法》《数据安全法》《个人信息保护法》等关键立法已经出台或正在加紧制定中。下一步，在《"十四五"规划建议》指导下，我国互联网法治建设将从细化重点法律制度、协调整体立法体系、探索新技术新应用立法等方面进一步充实法律制度，提高整体治理水平。同时，为应对复杂国际形势和数字全球化的需要，可以从数据跨境流动问题入手，积极参与和制定区域性规则，加强国际多双边合作和沟通机制建设。

（一）通过完善配套制度加快重点立法落地

当前，互联网法治体系建设初步完成，重要立法已经从整体上初步明确了互联网法治的顶层制度设计。下一步，在进一步推动《数据安全法》《个人信息保护法》制定出台基础之上，需要通过完善配套制度规定、修订重要立法和精细化立法适用等方式来推动互联网法治水平的整体提升。

一是通过完善重要立法的配套规定有效实现制度落地实施。《网络安全法》生效实施以来，当前仅在网络安全审查领域出台了《网络安全审查办法》，针对跨境数据流动、网络安全等级保护等重要制度

应当如何落地实施并没有明确的下位法支撑。另外，我国《数据安全法》和《个人信息保护法》也在加紧制定过程中，出台之后也涉及到的有关数据的诸多具体制度需要进行细化落实，尤其在疫情防控中，通过数字化举措开展相关工作产生的个人信息利用和公共利益的平衡、国家获取企业数据的权限和程序等问题需要进一步明确。下一步，在加快重要立法出台的基础上，将推动制定关键信息基础设施安全保护、数据跨境流动、数据分级分类、数据泄露通知、网络安全审查等重要制度的配套体系建设，通过更加细化的规定明确各项制度实施的关键要素、具体程序、具体要求等内容。

二是通过技术赋能提高网络执法水平。信息技术能力的提升使得弱信息技术时代难以规范的领域呈现被规范的可能，例如《网络信息内容生态治理规定》将网络内容从“二分法”调整为“三分法”，以抑制网上海量不良信息的泛滥。在此背景下，传统的执法手段难以快速识别不良信息，执法效果的准确性受到影响，而信息精准识别分析等筛查手段则能高效迅速的分辨不良信息，将其标签化，限制其传播。下一步，在确保安全前提下，需要积极探索利用信息赋能大规模拓宽网络空间规范领域，从多角度多层次规范网络空间。

三是个案析理提升立法清晰度。目前我国网络法治领域多为统筹性、原则性立法，在具体案件适用过程中存在出清晰性不足的问题。下一步，我国可以在复杂领域通过司法审判对具体案件进行法律适用的深入分析，摸清规则适用的现实影响，探索切实有效的规范样态，为法律修订奠定经验基础。

（二）结合产业发展明确重点领域立法趋势

过去一年，多地开展了前瞻性的数据立法探索，制定和公布了一批数据相关立法，如《深圳经济特区数据条例（征求意见稿）》《贵州省政府数据共享开放条例》《天津市数据交易管理暂行办法（征求意见稿）》的公布和出台明确了数据权、政府数据开放共享、数据交易等多项制度。地方先行立法的模式体现了各地政府试图以数据为主要抓手，构建促进数字经济发展的地方法治体系，但在数据产业方兴未艾、中央层面立法尚未制定的背景下，地方各自立法还应充分考虑产业发展诉求和避免条块状分割的问题。

一方面要处理好产业发展和立法之间的横向关系，循序渐进开展立法。立法是针对发展成熟的产业所存在的问题进行规制的手段，当前我国数据共享、数据交易等产业还处于初级探索阶段，虽然得到了国家和地方政府的支持，但是在平台性质、责任承担、行业标准等问题上，各方仍没有形成共识。如果在这一发展阶段直接采用“硬法”的形式进行规制，则可能产生压制企业创新发展的负面效果。下一步，针对数据交易等新兴产业，可以通过出台规范性文件、行业标准等“软法”的形式，以引导为主规范产业有序发展，先行推动各方在突出问题上统一标准、达成共识，同时密切关注和研究产业推进过程中伴生的相关挑战，在发展成熟阶段针对未能解决的问题再行研究制定出台相关立法。

另一方面要处理好地方立法和中央立法的纵向关系，避免立法条块分割问题。当前，中央在扶持和促进大数据产业发展方面仍以发布

政策性文件为主，并没有形成统一的立法。对于数据这种流动性要素来说，各地采取立法强规制模式，可能会带来地方保护主义盛行，条块分割，设置贸易壁垒等现象，由此影响国内市场统一及国家法制统一。企业在各地开展数据合规活动时也会面临因数据处理要求差异化而难以同时满足多方要求的客观障碍。下一步，首先应明确划分中央和地方在数据产业等互联网关键领域的立法权限问题，地方部门尽量应在已有上位法依据的前提下开展地方立法，如果没有上位法依据，在推动中央立法的基础上，地方部门还可通过适用传统立法、制定规范性文件或行业标准的方式解决问题，促进形成中央和地方良性互动、各地之间协调一致的有利局面。

（三）通过具体场景解决新技术新应用立法

人工智能、区块链、第五代移动通信（5G）以及物联网等新技术在各领域深度融合应用，不断催生出各种新产品、新业态、新应用，在极大提升效率、丰富人们选择的同时也带来了一系列新的安全和发展方面的问题，如人脸识别技术应用带来的个人隐私保护问题，算法自动化决策带来对特殊群体的歧视，自动驾驶汽车事故风险责任难以分配，互联网技术、商业模式、大数据等创新成果的知识产权保护等。在新技术融合交织、不断发展的背景下，政府部门往往难以使用统一的法律规则或技术标准进行规制，不恰当的立法或监管举措不仅难以保障相关主体的权益，还会在某种程度上限制产业发展。未来，应平衡新技术新应用中的发展与安全关系，针对不同方面的问题采取不同的规范方式。

一方面，根据应用场景、影响范围、可能的危害程度的不同，对新技术新应用风险采用分类治理的思路。**首先，**区分新技术新应用风险等级。可借鉴国际经验，将涉及国家安全、人民群众生命财产安全、社会稳定等领域设定为高风险领域，明确具体高风险应用场景。**其次，**对不同类型风险采取不同层级治理举措。对“高风险”的应用场景可采取风险规制思路，强化事前监管，对应用准入设置必要的评估等要求，完善相应责任立法体系；对一般应用领域可采取基于结果的规制思路，侧重于事中事后的监管，提升行业自律与技术标准的重要性。

另一方面，对知识产权保护不足、版权认定困难的问题进一步深入研究、提前布局。如各国对人工智能生成物所包含的权利类型和权利归属存有争议，人工智能创作物的版权保护仍普遍面临法律滞后问题。澳大利亚法院判定，利用人工智能生成的作品不能由版权保护，因为它不是人类制作的。如果人工智能创作物得不到法律有力的保护，会使得人工智能生成信息的复制和扩散门槛更低，影响投资人、创造人投入人工智能创作的积极性。

（四）通过整体机制促进数据安全有序流动

随着互联网新技术重塑生产、贸易和横跨其间的全球价值链，世界正在步入一个数字全球化新时代，与此相伴，数据跨境流动将逐步成为连接全球经济的纽带。当前，我国发布的海南、北京自贸港、自贸区方案中，均提出要创新跨境数据流动管理机制。2020 年 9 月，国务委员、外交部长王毅提出了《全球数据安全倡议》，反映了我国以安全为前提实现数据流动的态度。未来，我国将秉持发展和安全并

重的原则，以数据分级分类管理为抓手不断建立健全我国数据跨境流动管理机制。同时，在推动实现互利共赢、共同发展基础上，积极开展数据领域国际交流与合作，促进数据跨境安全、自由流动。

一是坚持发展和安全并重的原则。以安全为前提促进数据跨境自由流动已经逐步成为全球共识，既要坚持促进数据有序、自由流动，同时也不能忽略数据主权、个人信息保护等安全利益，下一步，在坚持国家整体数据安全、维护个人合法权益、保障产业利益等前提下，对数据跨境流动实施不同程度的管理，通过合理的制度设计保障具体场景下的数据安全，最大程度取得数字经济的发展利益和安全利益。

二是通过数据分级分类管理实现数据跨境流动的安全诉求。数据体量巨大、类型繁多，针对所有数据的跨境流动实施严格管理并不符合数字全球化的主导态势。当前大多数国家和地区的跨境数据流动监管主要针对个人数据、重要数据等类型，严格禁止跨境流动的类型主要是关键个人数据、物联网数据、金融数据等。未来数据跨境流动政策应避免采取“一刀切”模式，综合考虑具体场景中数据出境管理目的、范围、数量、类型等因素，通过对各个行业领域的数据进行细分，区分重要程度明确不同跨境监管政策。

三是通过多双边机制形成数据跨境流动区域性规则。由于各国间的利益和立场存在差异，目前还没有建立全球统一的数据跨境流动规则，价值观一致和贸易往来频繁的国家之间通过构建多双边机制促进相互之间的数据跨境流动，整体呈现区域性、模式差异化的显著特点。这一形式在较长时间内仍将是全球数据跨境流动的主要方式。下一步，

我国应充分发挥现有多边机制作用，在传统贸易伙伴基础上，扩大数据领域合作，依托“一带一路”、中欧等机制，参考刚刚签署的《区域全面经济伙伴关系协定》（RCEP），继续推进构建以我国为主导的区域性数据跨境流动规则。同时，跨境执法合作领域应在明确不得侵犯第三国司法主权和数据安全基本原则前提下，通过司法协助渠道或国家间相关双多边协议开展相关跨境调取数据工作。

附件一：过去一年网络法治大事记

一、《民法典》

入选理由：《民法典》是新中国第一部以法典命名的法律、是新中国截至目前体量最为庞大的法律，被誉为社会生活的百科全书。

法治影响：单独规定了人格权编，并在其中对“隐私”和“个人信息”进行了比较清晰的区分，对于《个人信息保护法》的制定具有重要的指导和借鉴意义。

二、《未成年人保护法》

入选理由：新增“网络保护”专章，填补了我国对未成年人网络沉迷、网络霸凌等互联网行为进行规制的法律空白。

法治影响：为我国《未成年人网络保护条例》的制定提供了明确的上位法依据。

三、《数据安全法（草案）》

入选理由：以法律形式填补了我国整体数据安全治理的空白，确立了我国数据安全工作的顶层设计制度，是国家安全工作的重要组成部分。

法治影响：为各部门各地区的数据安全立法和执法工作提供了上位法依据。

四、《个人信息保护法（草案）》

入选理由：开启了我国在个人信息保护领域进行统一立法的元年，具有重要的里程碑意义。

法治影响：有助于统一现行不同行业领域的个人信息保护相关规

定，有助于为国家机关的个人信息保护工作明确相关法律要求。

五、《网络信息内容生态治理规定》

入选理由：突破性的将网络内容的区分从“两分法”模式调整到了“三分法”模式。

法治影响：明确依法规范和管理平台上的违法信息、防范和抵制不良信息传播，是网络信息服务提供者必须承担的社会责任，也是法律责任。

六、《网络安全审查办法》

入选理由：是《网络安全法》生效以来的第一部配套规定，通过联合发布的方式体现了部门利益之间的协调。

法治影响：解决了网络安全审查工作法律适用的问题。

附件二：过去一年互联网立法梳理

层级	名称	发文字号	发布时间	生效时间
法律	中华人民共和国民法典	中华人民共和国主席令第 45 号	2020.05.28	2021.01.01
	中华人民共和国档案法(2020 修订)	中华人民共和国主席令第 47 号	2020.06.20	2021.01.01
	中华人民共和国未成年人保护法(2020 修订)	中华人民共和国主席令第 57 号	2020.10.17	2021.06.01
	中华人民共和国出口管制法	中华人民共和国主席令第 58 号	2020.10.17	2020.12.01
	中华人民共和国证券法(2019 修订)	中华人民共和国主席令第 37 号	2019.12.28	2020.03.01
	中华人民共和国基本医疗卫生与健康促进法	中华人民共和国主席令第 38 号	2019.12.28	2020.06.01
行 政法规	保障中小企业款项支付条例	中华人民共和国国务院令第 728 号	2020.07.05	2020.09.01
	中华人民共和国外商投资法实施条例	中华人民共和国国务院令第 723 号	2019.12.26	2020.01.01
部 门规章	网络信息内容生态治理规定	国家网信办令第 5 号	2019.12.15	2020.03.01
	网络预约出租汽车经营服务管理暂行办法(2019 修正)	中华人民共和国交通运输部令 2019 年第 46 号	2019.12.28	2019.12.28
	气象信息服务管理办法(2020 修正)	中国气象局令第 35 号	2020.03.24	2020.05.01
	网络安全审查办法	国家网信办、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电	2020.04.13	2020.06.01

		视总局、国家保密局、国家密码管理局令第 6 号		
	商业银行互联网贷款管理暂行办法	中国银行保险监督管理委员会令 2020 年第 9 号	2020.07.12	2020.07.12
	工业通信业行业标准制定管理办法	中华人民共和国工业和信息化部令第 55 号	2020.08.12	2020.10.01
	在线旅游经营服务管理暂行规定	中华人民共和国文化和旅游部令第 4 号	2020.08.20	2020.10.01
规范性文件	国家卫生健康委办公厅、国家中医药局办公室关于加强全民健康信息标准化体系建设的意见	国卫办规划发[2020]14 号	2020.09.27	2020.09.27
	国务院办公厅电子政务办公室、人力资源社会保障办公厅关于依托全国一体化在线政务服务平台做好社会保障卡应用推广工作的通知	国办电政函[2020]13 号	2020.03.03	2020.03.03
	国务院办公厅关于同意调整完善网络市场监管部际联席会议制度的函	国办函[2020]52 号	2020.07.08	2020.07.08
	文化和旅游部关于印发《游戏游艺设备管理办法》的通知	文旅市场发[2019]129 号	2019.11.06	2020.01.01
	国家知识产权局办公室关于印发《国家知识产权局政府信息公开实施办法(修订)》等文件的通知	国知办发办字[2019]43 号	2019.11.18	2019.11.18

	工业和信息化部关于印发《增强机器类通信系统频率使用管理规定(暂行)》的通知	工业和信息化部无[2019]248 号	2019.11.19	2020.01.01
	国家卫生健康委办公厅关于加强信息化支撑新型冠状病毒感染的肺炎疫情防控工作的通知	国卫办规划函[2020]100号	2020.02.03	2020.02.03
	中国人民银行关于发布《网上银行系统信息安全通用规范》行业标准的通知(2020)	银发[2020]35 号	2020.02.05	2020.02.05
	国家卫生健康委办公厅关于进一步推动互联网医疗服务发展和规范管理的通知	国卫办医函[2020]330 号	2020.04.18	2020.04.18
	工业和信息化部关于工业大数据发展的指导意见	工业和信息化部信发[2020]67 号	2020.04.28	2020.04.28
	国家网信办、文化和旅游部、国家广播电视总局关于印发《网络音视频信息服务管理规定》的通知	国信办通字[2019]3 号	2019.11.18	2020.01.01
	教育部等六部门关于联合开展未成.人网络环境专项治理行动的通知	教基[2020]6 号	2020.08.19	2020.08.19
	国家标准化管理委员会、中央网信办、国家发展改革委等关于印发《国家新一代人工智能标准体系建设指南》的通知	国标委联[2020]35 号	2020.07.27	2020.07.27
	农业农村部办公厅关于印发《2020 年农业农村部网络安全和信息化工作要点》的通知	农办市[2020]6 号	2020.05.07	2020.05.07

	工业和信息化部、公安部、国家标准化管理委员会关于印发《国家车联网产业标准体系建设指南(车辆智能管理)》的通知	工业和信息化部联科[2020]61 号	2020.04.15	2020.04.15
	国家发展改革委、中央网信办印发《关于推进“上云用数赋智”行动培育新经济发展实施方案》的通知	发改高技[2020]552 号	2020.04.07	2020.04.07
	国家发展改革委、中央网信办、科技部等关于印发《智能汽车创新发展战略》的通知	发改产业[2020]202 号	2020.02.10	2020.02.10
司法解释	《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释（三）》	法释〔2020〕10 号	2020.9.12	2020.9.14
相关标准	工业和信息化部批准《5G 移动通信网核心网总体技术要求》等 447 项行业标准	工业和信息化部		
	《个人金融信息保护技术规范》	中央人民银行	2020.2.13	
征求意见稿	《网络安全标准实践指南—移动互联网应用程序（App）个人信息安全防范指引（征求意见稿）》	全国信息安全标准化技术委员会	2020.3.30.	
	《网络数据安全标准体系建设指南》（征求意见稿）	工业和信息化部	2020.4.10.	
	《个人保险实名制管理办法（征求意见稿）》	中国银保监会	2020.4.24	

	《关于涉网络知识产权侵权纠纷有关法律适用问题的批复（征求意见稿）》	最高人民法院	2020.6.10.	
	《数据安全法(草案)》征求意见	全国人大常委会法制工作委员会	2020.07.03	
	《电信和互联网行业数据安全标准体系建设指南（征求意见稿）》	工业和信息化部	2020.08.10	
	《工业互联网标识管理办法》（征求意见稿）	工业和信息化部	2020.9.13.	.
	《互联网用户公众账号信息服务管理规定（修订草案征求意见稿）》	国家网信办	2020.10.15 .	
	《个人信息保护法（草案）》征求意见	全国人大常委会法制工作委员会	2020.10.22	
	《互联网直播营销信息内容服务管理规定（征求意见稿）》	国家网信办	2020.11.13	

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62302973

传真：010-62304980

网址：www.caict.ac.cn

